Order Code RS21727
February 5, 2004

Sensitive Security Information (SSI) and Transportation Security: Background and Controversies

Mitchel A. Sollenberger
Analyst in American National Government
Government and Finance Division

Summary

In November 2003, the U.S. attorney's office in Miami dropped a criminal case against a former federal baggage screener charged with stealing from a passenger's luggage. The case was dropped because prosecutors feared that sensitive security information (SSI) would have to be disclosed. At issue is the ability of the Transportation Security Administration (TSA) to prosecute other dishonest agency employees in the future. Will the same dilemma that led to the dismissal of this particular case occur again? In recent months, this and other important issues relating to SSI have been raised. This report provides a brief background on SSI regulation, an overview of the current policy issues, and a description of the criticism of, and support for, SSI policy. This report will be updated as events warrant.

Background

On November 16, 2001, 63 days after the attacks on the World Trade Center and the Pentagon, Congress passed the Aviation and Transportation Security Act (ATSA); and the President signed it into law on November 19, 2001.[1] Congress enacted ATSA to increase aviation security after the September 11 terrorist attacks. Under ATSA, Congress created the Transportation Security Administration (TSA) and authorized the agency to make improvements in the country's transportation security.[2] Based on this authority, the Under Secretary of Transportation for Security transferred authority for the

[1] S. 1447, 107th Cong., P.L. 107-71. See also U.S. President (G. W. Bush), "Remarks on Signing the Aviation and Transportation Security Act," *Weekly Compilation of Presidential Documents*, vo1. 37, Nov. 19, 2001.

[2] The act directs TSA to prescribe rules and regulations to protect individuals and property on aircraft. See 49 U.S.C. 44903 et seq.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
05 FEB 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Sensitive Security Information (SSI) and Transportation Security: Background and Controversies	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library, and Knowledge Repository Defense Acquisition University Fort Belvoir, VA 22060**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**6**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

existing Federal Aviation Administration regulations,[3] which include SSI, to the Transportation Security Administration[4] on February 22, 2002.[5] The TSA incorporated these regulations into its Transportation Security Regulations (TSRs).

The TSRs contain rules on administration, procedure, and security for air, land, and maritime transportation. Subchapter A, titled "Administrative and Procedural Rules," contains Part 1520, which addresses Sensitive Security Information (SSI). The *Federal Register* notice on the regulations describes or defines SSI as including "information about security programs, vulnerability assessments, technical specifications of certain screening equipment and objects used to test screening equipment ... and other information."[6] This definition is spelled out in more detail in 49 C.F.R. 1520.7, which is summarized below.

- Section 1520.7(a) protects any security program "that relates to United States mail to be transported by air."
- Section 1520.7(b) through (d) covers security directives and information circulars, selection criteria used in the security screening process, and security contingency plans and/or instructions pertaining to those plans.
- Section 1520.7(e) through (g) relates to any technical specification of any device or equipment used for security communications, screening, or "detecting deadly or dangerous weapons," including an "explosive, incendiary, or destructive substance."
- Section 1520.7(h) covers the release of information that TSA "has determined may reveal a systemic vulnerability of the aviation system, or a vulnerability of aviation facilities, to attack."
- Section 1520.7(i) protects "information [released by TSA] concerning threats against transportation."
- Section 1520.7(j) protects "details of aviation security measures."
- Section 1520.7(k) and (l) relates to any "information" TSA has prohibited from disclosure under the criteria of 49 U.S.C. 40119, or any draft, proposed, or recommended change to the information or records identified in this section.
- Section 1520.7(m) through (p) covers locations, tests, and scores of tests on all screening methods or equipment.
- Section 1520.7(q) protects "images and descriptions of threat images for threat projection systems."
- Section 1520.7(r) relates to all Department of Transportation information on "vulnerability assessment ... irrespective of mode of transportation."

---

[3] Title 14, Code of Federal Regulations (C.F.R.), Parts 91, 107, 108, 109, 121, 129, 135, 139, and 191.

[4] Title 49 C.F.R., Parts 1500, 1520, 1540, 1542, 1544, 1546, 1548, and 1550.

[5] The final rule was published in the Feb. 22, 2002 edition of the *Federal Register*. See U.S. Department of Transportation, "Civil Aviation Security Rules," *Federal Register*, vol. 67, no. 36, Feb. 22, 2002.

[6] Ibid., p. 8342.

Section 1520.5 specifies that all airport operators, aircraft operators, foreign air carriers, indirect air carriers, applicants, and other persons who receive SSI must protect that information from disclosure. SSI may be exempted from disclosure under the Freedom of Information Act.[7]

Controversies

The regulations are intended to reduce the risk of vital security information reaching the wrong hands and resulting in another terrorist attack. The regulations governing SSI, however, have raised a number of concerns about the management of such information and the accountability of governmental agencies. This section highlights four cases that have surfaced over the last two years, in which the SSI regulations were applied to withhold information. The cases deal with airport security procedures, employee accountability, passenger screening, and airport secrecy agreements.

In January 2003, the Dallas/Fort Worth Airport experienced an early controversy involving TSA security procedures. The incident involved a federal screener who permitted a man to pass through security after his luggage tested positive for an explosive. The airport was closed for over an hour while TSA and law enforcement authorities searched for the individual. After the incident, a TSA spokesman stated that the agency was "not going to be issuing any kind of report because anything beyond the most general of comments would lead us into areas which concern sensitive security information."[8] The use of SSI rules to prevent the release of information has raised the concerns of some experts. For example, Jane E. Kirtley, director of The Silha Center for the Study of Media Ethics and Law at the School of Journalism and Mass Communication at the University of Minnesota has stated, "The public has a burning interest in knowing how secure the nation's airports are. It is not satisfactory in a democracy to say when an incident happens that we're taking care of the problems."[9] On the other hand, some have argued that the release of certain information could harm the public. The TSA has stated "if [SSI] information were to fall into the wrong hands it could be used to attack the transportation system."[10]

A second controversy arose when the U.S. attorney's office in Miami dropped a criminal case against a former federal baggage screener who was charged with stealing

---

[7] 49 U.S.C. 40119(b)(1). In cases where a person is facing a charge of violating TSA security regulation(s), the alleged violator may be provided copies of the enforcement investigative report which may contain SSI. See 49 C.F.R. 1520.3(d).

[8] Terri Langford, "Report on Incident at D/FW is Sealed; Agency Cites Security in Withholding Details on Breach, Evacuation," *The Dallas Morning News*, Jan. 24, 2003, p. 30A.

[9] Bryon Okada, "Public Will Not Be Told Details of D/FW Breach," *Fort Worth Star-Telegram*, Jan. 24, 2003, p. 1. For further reading on Executive Branch secrecy see, Jane E. Kirtley, "The American Executive Branch: A Culture of Secrecy," in *The Long Term View*, Lawrence R. Velvel and Holly Vietzke, eds. vol. 6, fall 2003, pp. 43-49.

[10] Sara Kehaulani Goo, "TSA Faulted for Restricting Information," *The Washington Post*, Oct. 10, 2003, p. A11.

from passengers in November 2003.[11] The U.S. attorney's office withdrew the charges because a federal judge determined that the defense could cross-examine the prosecution's witnesses, which could raise the possibly of disclosing SSI about TSA's security and training procedures. The problem with the decision of the Justice Department according to a TSA spokeswoman, is that "future prosecutions of dishonest agency employees would be hamstrung by the same dilemma that led to the dismissal of the indictment."[12] The public defender in the case suggested that "prosecutors could have drop[ped] the part of the conspiracy charge relating to the sensitive security information ... and [moved] forward with the other two underlying offenses — breaking into baggage and stealing their contents."[13] The U.S. attorney's office and TSA, however, decided the risk of releasing SSI was too great.

A third controversy involves the Computer Assisted Passenger Pre-Screening system (CAPPS). In the summer of 2004, TSA plans to update the system and call it CAPPS II.[14] The original CAPPS system attempted to screen passengers by "focusing primarily on travel patterns and financial transactions."[15] The new system, in addition to monitoring travel records, will check various personal records of passengers trying to make reservations. These records, combined with "CIA, FBI, and other intelligence databases", will be used to select certain travelers for additional screening. Then-TSA Administrator Loy stated, "I don't think there is a single project that will do more potential good for aviation security." The system will be able "to trace would-be terrorists, even if they lead apparently unremarkable lives."[16] Some do not agree the system will function as TSA believes.[17] David Sobel of the Electronic Privacy Information Center thinks that CAPPS II is a "Catch-22" that will "present enormous challenges for clearing names — and an enormous temptation for misuse." For example, if a person is flagged by the system, Sobel says they "are going to want to know, 'Why am I pulled aside every time I take a flight?'" Since the system will contain SSI, the answer will be "Sorry, we can't tell you."[18]

---

[11] *USA v. Washington, et al*, PACER Service Center, 03-CR-20648-ALL, Nov. 13, 2003.

[12] Quoted in Dan Christensen, "Caught on Video Procedures 'Fair Game'," *Miami Daily Business Review*, Nov. 7, 2003, p. 12.

[13] Ibid.

[14] U.S. Department of Homeland Security, Transportation Security Administration, "TSA's CAPPS II Gives Equal Weight to Privacy Security," March 11, 2003, TSA 03-04, [http://www.tsa.gov/public/display?content=09000519800193c2], visited Jan. 4, 2004.

[15] Ricardo Alonso-Zaldivar, "Airport Security Flaws Bring Criticism," *Los Angeles Times*, July 2, 2002, p. A8.

[16] Charles Piller and Ricardo Alonso-Zaldivar, "A Suspect Computer Program; The Government is Working to Better Screen Airline Travelers," *Los Angeles Times*, Oct. 2, 2003, p. 1.

[17] Due to the primary concentration on passenger's air travel records, instead of personal information, the original CAPPS system did not receive the same attention as CAPPS II. For information on the CAPPS II and similar databases see CRS Report RL31798, *Data Mining: An Overview*, by Jeffrey W. Seifert.

[18] Piller and Alonso-Zaldivar, "A Suspect Computer Program," p. 1.

TSA officials point out that "a passenger advocate and appeals process" will be available when the system goes online.[19]

A fourth SSI controversy involves a security agreement between airport administrations, local police departments, and TSA officials. The agreements prohibit the local police from commenting on any incident involving SSI that has occurred on airport property without authorization by the proper TSA officials. Failure to comply with the agreement may mean the loss of financial aid for airport security.[20] A partial copy of one of the agreements contains the following two sections.

> A copy of any summons, complaint, subpoena or other legal document served upon a local law enforcement organization that is related to a local proceeding that seeks records or testimony containing sensitive security information shall be promptly forwarded to the ... Transportation Security Administration field counsel.
>
> All media releases and other contact with or by media specific to the security directive, ... the airport security program, or other subsequent or superceding regulations or documents regarding law enforcement services for aviation security shall be coordinated with the federal security director or the federal security director's designee. All media releases and other contact with or by media on the terms and conditions of this reimbursement agreement shall be coordinated with the contracting officer.[21]

When these agreements were initially designed, many local officials reportedly were not sure of the exact level of compliance they required. For example, police officials in Des Moines, IA, thought that they might be prevented from discussing with the public "a bomb or shooting incident at the airport." The local police chief, William McCarthy, reasoned that the "agreement may even prevent officers from 'reporting the arrest of a drunk at the airport'" or testifying in court without clearance from TSA.[22]

Only after Iowa Senators Charles Grassley and Tom Harkin became involved in the matter was the agreement clarified. In a letter to Senator Grassley, TSA Administrator James Loy explained that the agreement was not a "gag order" for local police, but was intended to inform TSA officials about incidents that occur on airport property. In addition, Loy stated "that law enforcement officers who are asked to testify about purely factual matters that do not reveal sensitive [security] information may do so without

---

[19] Ibid. TSA is creating the new Passenger Advocate's Office to "work with and on behalf of passengers to identify and correct any erroneous data that may have been utilized in the authentication or risk assessment modules." See U.S. Department of Homeland Security, Transportation Security Administration, "CAPPS II Fact Sheet," Sept. 29, 2003, [http://www.tsa.gov/public/display?content=0900051980057f66], visited Jan. 30, 2004.

[20] See Tom Alex, "Secrecy in Airport Security Contract Criticized," *Des Moines Register*, Sept. 27, 2003, p. 1A; James Andrews, "Here in Tristate, Security's Tighter; Everything Else is Wait-And-See," *The Cincinnati Enquirer*, March 19, 2003, p. 1A; and, Sara Kehaulani Goo and Carrie Johnson, "Police Searching Cars at Random Outside Airports," *Washington Post*, Feb. 19, 2003, p. A1.

[21] Provisions of the Des Moines security agreement as quoted in Alex, "Secrecy in Airport Security Contract Criticized," p. 1A.

[22] Quoted in ibid.

consultation with the federal government." The TSA letter also explained that copies of the agreement could be made public except for parts with sensitive security information, such as "Appendix A, which concerns the amount of airport security."[23]

Currently, the Des Moines issue has been resolved between TSA and local police. Lt. David Huberty of the Des Moines police department has stated that, since the clarification of the agreement, SSI has not been an issue. In fact, local police and TSA officials have a good working relationship. The close interaction between local and federal authorities in Des Moines, according to Lt. Huberty, has provided the airport-assigned police officers with a working understanding of SSI.[24] For example, incidents that occur on airport grounds outside the terminal are not generally reported to TSA officials since local police understand that they do not involve SSI. Incidents that do occur within the terminal or at checkpoints, however, are treated differently in that TSA officials are involved and local police will write up more generalized descriptions of the incident so that SSI is not revealed.[25] In addition, a TSA attorney will provide a training seminar for the Des Moines police department to better understand the SSI regulation.[26]

Conclusions

The implementation of SSI regulations has created a number of controversies for TSA. The agency has worked to alleviate these concerns, but some experts are not convinced. They are still alarmed that SSI is currently "muzzling debate of security measures,"[27] and although they acknowledge that some information should be kept secret, "the refusal to release other information seems overzealous." For example, according to Paul S. Hudson of the Aviation Consumer Action Project, at a recently held aviation meeting, information in one report was labeled SSI and prevented participants from having "any exchange of views."[28] For some, the issue being raised is the need for security versus the public's right to know. This issue, Kirtley contends, comes down to whether "our openness was what made us so vulnerable."[29] SSI justifications are not made on those grounds, but the TSA warns that SSI would "be damaging to the security of the [airline] industry and could well be damaging to the security of the United States were it to be publicly disclosed."[30] SSI will continually be discussed in a post 9/11 environment where the TSA has to weigh its duty to provide air, land, and maritime security against the need to keep the public informed and maintain constitutional rights and safeguards.

---

[23] Tom Alex, "Dispute Settled on Airport Pact," *Des Moines Register*, Nov. 13, 2003, p. 6B.

[24] Lt. David Huberty, Des Moines Police, telephone conversation with the author, Dec. 4, 2003.

[25] Ibid. Lt. Huberty said that the generalized reports are needed because, for instance, information concerning how weapons were discovered would not be released because TSA procedures are classified as SSI.

[26] Ibid.

[27] Goo, "TSA Faulted for Restricting Information,"p. A11.

[28] Ibid.

[29] Okada, "Public Will Not Be Told Details of D/FW Breach," p. 1.

[30] Angela Greiling Keane, "Search for Answers: Recommendations for Air Cargo Security Being Drafted in Secret by 14-Year Old Advisory Panel," *Traffic World*, May 12, 2003, p. 14.